Table of contents

[1. Introduction 2](#_Toc478025672)

[1.1 Context 2](#_Toc478025673)

[1.2. Background 2](#_Toc478025674)

[1.3. Problem and research question 3](#_Toc478025675)

[2. Related works 4](#_Toc478025676)

[3. Methodology employed 6](#_Toc478025677)

[4. Results found and perspectives 8](#_Toc478025678)

[5. Most important publications for this work 10](#_Toc478025679)

# 1. Introduction

## 1.1 Context

Phising attacks address weaknesses in systems due to the human factor. Several cyber attacks have spread by exploiting the vulnerabilities found at the end-user level, making the user the weakest element of the security chain. For example, a system can be very secure from the technical side against attacks, but end users may ignore giving their password if a hacker asks them to change their password via any site, For example users who have the reflex to put their password of an account after an email address, on forms where the email and the password are requested.

On the other hand, hackers can use technical vulnerabilities (for example, DNS poisoning) to build much more persuasive socially designed messages (ie, the use of legitimate but falsified domain names may seem much more compelling than the " Use of another domain name). All this makes phishing attacks a stratified problem and effective mitigation would require addressing both technical and human problems.

Because phising attacks are designed to exploit weaknesses among end-users of the system, it is often difficult to mitigate them because few users are able to detect them.

## 1.2. Background

According to APWG, the term phishing was invented in 1996 due to social engineering attacks against America Online (AOL) accounts by online scammers, stolen accounts via phishing attacks have also been used as a Between hackers before 1997 for trade in piracy software in exchange for stolen accounts. Phishing attacks have been historically started by theft of AOL accounts, and over the years have begun to attack more profitable targets, such as online banking and e-commerce services.

Currently, phishing attacks target not only the end users of the system, but also the technical employees of service providers, and can deploy sophisticated techniques such as MITB attacks.

## 1.3. Problem and research question

Because the phishing problem takes advantage of human ignorance or naivete in their interaction with electronic communication channels (eg E-Mail, HTTP, etc.), it is not a Problem easy to solve permanently. All the proposed solutions attempt to minimize the impact of phishing attacks. From a high-level perspective, there are usually two commonly proposed solutions to mitigate phishing attacks:

* education of the user; Human is instructed in an attempt to improve its classification accuracy to correctly identify phishing messages and then apply appropriate actions on properly classified phishing messages, such as attacks notifying system administrators.
* Software improvement; The software is enhanced to better classify phishing messages on behalf of humans or to provide information in a more obvious way so that humans are less likely to ignore them.

The challenges with both approaches are:

* Non-technical people resist learning, and if they learn they do not retain their knowledge permanently, and therefore training should be done continuously.
* Some software solutions, such as authentication and security warnings, are always dependent on the behavior of the user. If users ignore the security warnings, the solution may be rendered unnecessary.

# 2. Related works

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Detection Technique/author(s)** | **Blacklists** | **Whitelists** | **Heuristics** | **Visual Similarity** | **Machine Learning** | **Network Communication** | **False Positives** | **False Negatives** |
| PhishNet / P. Prakash, M. Kumar, R. R. Kompella, and M. Gupta |  |  |  |  |  |  | 5% | 3% |
| AIWL / Y. Cao, W. Han, and Y. Le |  |  |  |  |  |  | 0% | 0% |
| SpoofGuard / N. Chou, R. Ledesma, Y. Teraguchi, and J. C. Mitchell |  |  |  |  |  |  | 38% | 9% |
| CIDS / C. V. Zhou, C. Leckie, S. Karunasekera, and T. Peng |  |  |  |  |  |  | -- | -- |
| PhishGuard / P. Likarish, D. Dunbar, and T. E. Hansen |  |  |  |  |  |  | -- | -- |
| PhishCatch / W. D. Yu, S. Nargundkar, and N. Tiruthani |  |  |  |  |  |  | 1% | 20% |
| PhishWish / D. L. Cook, V. K. Gurbani, and M. Daniluk |  |  |  |  |  |  | 8.3% | 2.5% |
| CANTINA / Y. Zhang, J. I. Hong, and L. F. Cranor |  |  |  |  |  |  | 3% | 11% |
| A phishing sites blacklist generator / M. Sharifi and S. H. Siadati |  |  |  |  |  |  | 9% | 0% |
| Fighting phishing with discriminative keypoint features of webpages / K.-T. Chen, J.-Y. Chen, C.-R. Huang, and C.-S. Chen |  |  |  |  |  |  | <0.1% | <0.1% |
| Automatic Detection of Phishing Target from Phishing Webpage / M. Hara, A. Yamada, and Y. Miyake |  |  |  |  |  |  | 3.4% | 8.56% |
| Detecting DNS-poisoning-based phishing attacks from their network performance characteristics / G. Liu, B. Qiu, and L. Wenyin |  |  |  |  |  |  | 0.7% | 0.6% |
| **Detection Technique/author** | **Blacklists** | **Whitelists** | **Heuristics** | **Visual Similarity** | **Machine Learning** | **Network Communication** | **False Positives** | **False Negatives** |
| Textual and Visual Content-Based Anti-Phishing: A Bayesian Approach / H. Kim and J. Huh |  |  |  |  |  |  | 0-0.02% | 0-1.95% |
| Large-scale automatic classification of pages / C. Whittaker, B. Ryner, and M. Nazif |  |  |  |  |  |  | 0% | 16-30% |
| B-APT / P. Likarish, D. Dunbar, and T. E. Hansen |  |  |  |  |  |  | 3% | 0% |
| EBDIS / A. Stone |  |  |  |  |  |  | 1.9% | 25% |
| Detecting phishing emails using hybrid features / L. Ma, B. Ofoghi, P. Watters, and S. Brown |  |  |  |  |  |  | -- | -- |
| Model-based features / A. Bergholz, J. De Beer, S. Glahn, M.-F. Moens, G. Paaß, and S. Strobel |  |  |  |  |  |  | 0% | 1% |
| R-Boost / F. Toolan and J. Carthy |  |  |  |  |  |  | 1.4% | 0% |

# 3. Methodology employed

Due to the general nature of the phishing problem, it is important to visualize the life cycle of phishing attacks, and based on what classifies anti phishing solutions. We describe the life cycle of phishing campaigns from the point of view of anti-phishing techniques, which is supposed to be the most complete phishing solution flowchart. When a phishing campaign is launched (for example, by sending phishing emails to users), the first line of protection detects the campaign. Detection techniques are broad and could integrate the techniques used by service providers to detect attacks, classify end-user client software, and user awareness programs. The ability to detect phishing campaigns can be improved every time a phishing campaign is detected by learning from this experience. For example, by learning from previous phishing campaigns, it is possible to improve the detection of future phishing campaigns. Such learning can be performed by a human observer or software (ie via an automatic learning algorithm).

Once the phishing attack is detected, a number of actions could be applied to the campaign. According to our analysis of the literature, the following categories of approaches exist:

* Offensive defense - these approaches are aimed at attacking phishing campaigns to make them less effective. This approach is particularly useful for protecting users who have submitted their personal data to attackers.
* Correction approaches mainly focus on phishing suppression. In the case of phishing sites, this is possible by suspending the hosting account or by removing the phishing files.
* Prevention - phishing prevention methods are defined differently in the literature depending on the context. Here the goal is to try to prevent attackers from launching phishing campaigns in the future.

However, if the phishing campaign is not detected (whether detected by a user or a software classifier), none of these actions can be applied. This underscores the importance of the detection phase. We consider any anti-phishing solution that aims to identify or classify phishing attacks as detection solutions. This includes:

* User training approaches - end-users can be trained to better understand the nature of phishing attacks, which ultimately leads them to correctly identify phishing and non-phishing messages. However, user training approaches are aimed at improving end-users' ability to detect phishing attacks, and we therefore classify them under "detection".
* Software classification approaches - these mitigation approaches aim to classify phishing and legitimate messages on behalf of the user in order to close the gap that remains due to human error or ignorance. This is an important gap to be filled as user training is more costly than automated software classifiers, and user training may not be feasible in some scenarios (such as when the user base is enormous , Such as PayPal, eBay, etc.).

The performance of detection approaches can be improved during the learning phase of a classifier (whether the classifier is human or software). In the case of end-users, their classification capacity can be improved by improving their knowledge of phishing attacks by learning individually through their online experience or through external training programs. In the case of software classifiers, this can be done during the learning phase of a classifier based on machine learning, or the improvement of detection rules in a rule-based system.

# 4. Results found and perspectives

User education is an attempt to increase the level of technical awareness of users to reduce their vulnerability to phishing attacks. However, the human factor is broad and education alone can not guarantee a positive behavioral response. We understand that the user training approach is not always the right answer. However, it should be noted that user education can complement software solutions. However, it should also be noted that none of the existing studies empirically show sufficient evidence that user education can virtually complement software solutions. This is due to the fact that all publicly available education studies have evaluated educational materials independently of software solutions.

The works of *S. Sheng, M. Holbrook, P. Kumaraguru, LF Cranor, and J. Downs, "which falls for phish: a demographic analysis of phishing susceptibility and effectiveness of interventions," in Proceedings of the 28th Conference International,* *human factors in computer systems* have found that Anti-Phishing training material reduced the rate of False Negative from 46% to 29%, which is not enough evidence to suppose that it would also complement software solutions Which, for example, reach rate of False Negative of less than 1%. The question of non-response is: what is the percentage of overlap between end-user ranking after a user training phase and ranking by a software classifier? If the overlap is 100% then the addition of user training may be redundant and will not be worth the cost and complexity. However, if the overlap is less than 100%, then they may be complementary to each other. However, such a study are not available in the public literature. This survey examined a number of anti-phishing software techniques. Some of the important aspects in measuring phishing solutions are:

* detection accuracy with regard to zero-hour phishing attacks. This is due to the fact that phishing websites are essentially short-lived and detection at zero time is critical.
* Low false positives. A system with high false positives could cause more harm than good. In addition, end users will usually ignore safety warnings if the classifier is often confused.

In general, software detection solutions are:

* Blacklists.
* heuristics based on rules.
* visual similarity.
* Machine Learning based classifiers.

The results of the studies show that the use of machine learning techniques is promising as they have led to the most effective phishing classifiers in the literature known to the public. Detection techniques based on automatic learning achieve a high classification accuracy for the analysis of data pieces similar to those of heuristic rules-based techniques.

As future work in this field, it would be useful to conduct studies such as:

* measure the effect of adding user training from the point of view of correcting software classification errors.
* Analyze phishing detection techniques from the point of view of their consumption of cost and energy calculations.

# 5. Most important publications for this work

1. S. Sheng, M. Holbrook, P. Kumaraguru, LF Cranor, et J. Downs, " qui tombe pour phish ?: une analyse démographique de phishing susceptibilité et effectiven ess des interventions, " dans Actes de la 28 e conférence internationale sur l' homme facteurs dans les systèmes informatiques , ser. CHI ' 10. New York, NY, USA: ACM, 2010, pp 373. - 382.
2. C. Whittaker, B. Ryner, un e M. Nazif, " classification automatique à grande échelle des pages de phishing, " en SNSD ' 10 2010.
3. P. Kumaraguru, Y. Rhee, A. Acquisti, LF Cranor, J. Hong, et E. NUNGE, « La protection des personnes de phishing: la conception et l' évaluation d'un trai embarqué ning système de courrier électronique, " dans Actes de la conférence sur SIGCHI les facteurs humains dans les systèmes informatiques , ser. CHI ' 07. New York, NY, USA: ACM, 2007, pp 905. - 914.
4. S. Gorling, « Le mythe de l' utilisateur de l' éducation, " Actes de la 16e Virus B ulletin Conférence internationale 2006.
5. S. Sheng, B. Wardman, G. Warner, LF Cranor, J. Hong, et C. Zhang, " Une analyse empirique des listes noires de phishing, " dans Actes de la 6e Conférence Courriel et Anti-Spam , ser. CEAS ' 09, Vue sur la montagne, CA, Juillet 2009.
6. P. Likarish, D. Dunbar et TE Hansen, " PhishGuard: Un plug-in navigateur pour la protection contre le phishing, " en 2 e Conférence internationale sur Internet Multimedia Service Arc hitecture et Applications, 2008. IMSAA 2008 , 2008, pp 1. - 6.
7. Y. Zhang, JI Hong, et LF Cranor, " Cantina: une approche basée sur le contenu de détection des sites Web de phishing, " dans Actes de la conférence internationale sur le 16e World Wide Web , ser. WWW ' 07. New York, NY, USA: ACM, 2007, pp. 639 - 648.
8. L. Cranor, S. Egelman, J. Hong, et Y. Zhang, " Phinding phish: Une évaluation des barres d'outils anti-phishing, " www.cylab.cmu.edu/files/cmucylab06018.pdf, 2006, accessibles octobre 2011.